REMARKS/ARGUMENTS

I. Introduction:

Claim 31 is withdrawn from consideration. Claim 1 has been amended and claims 32-35 have been amended to depend from claim 18. With entry of this amendment, claims 1, 3-4, 6-21, 23-30, and 32-36 will be pending.

II. Claim Rejections Under 35 U.S.C. 103:

Claims 1, 3-4, 6-7, 9-11, 15-18, 20-21, 25, 27, and 36 stand rejected under 35 U.S.C. 103(a) as being unpatentable over WO 97/24841 (Cheriton et al.) in view of U.S. Patent No. 6,321,338 (Porras et al.)

Claim 1 is directed to a method for generating filters based on data entering a network device. The method includes: classifying network flow based on one or more packets received at the network device; performing a lookup based on the classified network flow and building a new flow cache entry if the lookup is unsuccessful; sending each of said network flows to a corresponding flow cache and implementing policies designated for each of said network flows; creating an aggregate network flow summary for each of said network flows; analyzing at least one of said aggregate network flow summaries to detect characteristics of potentially harmful network flows; and generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through the network device. Claim 1 further includes classifying network flows, performing a lookup, and creating an aggregate network flow summary. Claim 1 has been amended to clarify that a separate aggregate network flow summary is created for each network flow.

Cheriton et al. disclose datagram transmission over virtual circuits. The invention of Cheriton et al. is directed to providing support for a wide range of network transmission speeds and a wide variety of source traffic behavior, while maintaining compatibility with existing network protocols and applications. The system processes network datagram packets in network devices as separate flows, based on the source and destination address pair contained in the datagram packet. This allows the network to control and manage each flow of datagrams in a segregated manner. Processing steps that can be specified for each flow include traffic management, flow control, packet forwarding, access control, and other network management functions.

As noted by the Examiner, the Cheriton et al. PCT application does not show or suggest creating an aggregate network flow summary for each network flow, analyzing at least one of the aggregate network flow summaries to detect characteristics of potentially harmful network flows, or generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through the network device.

Porras et al. disclose a network surveillance system which receives network packets and builds a long-term and short-term statistical profile from a measure of the network packets that monitors data transfers, errors, or network connections. A comparison of statistical profiles is used to determine whether the difference between the statistical profiles indicates suspicious network activity. A service monitor provides records, which contain accumulated network traffic statistics (e.g., number of packets and number of kilobytes transferred).

Applicant respectfully submits that neither Cheriton et al. nor Porras et al., either alone in combination, show or suggest creating an aggregate network flow summary for separate network flows, analyzing aggregate network flow summaries, and generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through a network device.

The system of Porras et al. receives network packets at a device and examines the packets to provide statistical profiles. A service monitor is provided at a network device to monitor one stream of data packets entering the device. The data packets are not separated into separate flows, therefore, there is no need to create an aggregate network flow summary for different flows, as required by claim 1. Furthermore, Porras et al. examine all incoming packets rather than creating an aggregate network flow summary and analyzing at least one of the aggregate network flow summaries. The method of applicant's invention, as set forth in claim 1, allows network flows to be analyzed and information on incoming packets provided without examining each packet received. Flow collection aggregation allows data to be stored by aggregate summary records instead of raw data records.

Furthermore, claim 1 sets forth a method for generating filters based on data entering a network device and requires generating a filter to prevent packets corresponding to detected potentially harmful network flows from passing through the network device, whereas Porras et al. use enterprise monitors to focus on network attacks. The system of Porras et al. includes service monitors (16a-16c), which collect data at a network device (Fig.1). The service monitors disseminate information to domain monitors (16d-16e) and enterprise monitors 16f. Countermeasures for an attack include report dissemination to other monitors or administrators or severing a communication channel or reconfiguring logging facilities. The monitors may invoke probes to gather additional information about the source of suspicious traffic. Porras et al. do not teach generating a filter at the network device based on data entering the network device.

Accordingly, claim 1 is submitted as patentable over Cheriton et al. and Porras et al.

Claims 3-4, 6-14, and 23-27, depending either directly or indirectly from claim 1, are submitted as paten table for the reasons discussed above with respect to claim 1.

Claim 7 is further submitted as patentable over Cheriton et al. and Porras et al., which do not show or suggest propagating a filter generated at a network device, which collects and analyzes flow, to an upstream network device. As previously discussed, Porras et al. do not disclose generating a filter at the network device examining packets. In rejecting claim 7, the Examiner refers to col. 2, lines 54-60 of the Porras et al. patent. This section of the patent merely discusses how a monitor (domain monitor or enterprise monitor) that collects event reports from different monitors (service monitors) may correlate activity to identify attackers in more than one network entity.

Claim 15 is directed to a computer program product for generating filters based on analyzed network flows. The product generally comprises: code that separates data into different network flows and creates an aggregate network flow summary for one or more of the network flows; code that selects one or more network flows for analysis and analyzes the selected network flows by reviewing the aggregate network flow summaries; and code that detects potentially harmful network flows and automatically generates a filter to prevent packets corresponding to the detected potentially harmful network flows from passing through the network device. Claim 15 further includes code that creates an aggregate network flow summary for network flows. Claim 15 is submitted as patentable for the reasons discussed above with respect to claim 1.

Claims 16, 17, and 36, depending either directly or indirectly from claim 15, are submitted as patentable for the same reasons as claim 15.

Claim 17 is further submitted as patentable because neither Cheriton et al. nor Porras et al. show or suggest code that propagates a filter to an upstream network device. In rejecting claim 17, the Examiner refers to col. 8, lines 47-65. This portion of the patent sets forth a description of a resolver that operates as the center of intramonitor communication, and sets forth an example of how a service monitor report can be sent to an enterprise monitor. Porras et al. describe how a report produced by a service monitor 16a-16c in one domain could be propagated to an enterprise monitor 16f, which in turn sensitizes service monitors in other domains to the same activity. Porras et al. do not

send a filter generated at a network device to an upstream network device. Instead, Porras et al. send information from a network device to another device which in turn passes the information onto other network devices in different domains.

Claim 18 is directed to a system for automatically generating filters based on data entering a network device and is submitted as patentable for the reasons discussed above with respect to claim 1. Claims 19-21 and 32-35, depending either directly or indirectly from claim 18, are submitted as patentable for the same reasons as claim 18.

Furthermore, claim 21 is submitted as patentable for the reasons discussed above with respect to claims 7 and 17.

Claims 8 and 19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton et al. and Porras et al in view of U.S. Patent No. 6,266,706 (Brodnik et al.). Brodnik et al. describe a fast routing lookup system. In rejecting these claims, the Examiner refers to col.2, line 64- col. 3, line 3 of the Brodnik et al. patent. In this prior art section, Brodnik et al. note that IP router designs use special-purpose hardware to do IP processing. However, Brodnik et al. go on to describe how this can be an inflexible solution since any changes in the IP format or protocol could invalidate such designs and the flexibility of software makes it a more preferable solution. Brodnik et al. also note that using hardware to do routing lookups is an expensive solution. Brodnik et al. thus, teach away from using hardware to send each network flow to a corresponding flow cache. Accordingly, claims 8 and 19 are submitted as patentable over Brodnik et al. and the other prior art of record.

Claim 23 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton et al. and Porras et al. in view of "Live Traffic Analysis of TCP/IP Gateways" (Valdes et al). in further view of Brodnik et al. As discussed above, Brodnik et al. do not teach using hardware to reduce information so that flow records can be analyzed by software. Valdes et al. also do not disclose reducing information resulting from analyzing data in hardware so that data can be analyzed in software.

Claims 24 and 28-30 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton et al. and Porras in view of Application Note 2037 "Nemesis Firewall" (Allied Telesyn). The Allied Telesyn application note merely points out that in order to refine security policy, rules can be added to deny or allow access based on various parameters. This reference does not remedy the deficiencies of the primary references. Claim 24 provides for further refinement of the generated filter. Thus, once a group of packets are identified as harmful, the corresponding network flows can be analyzed to further refine the filter. Instead of filtering out all data arriving from an identified organization, only destructive packets received from an actual attacker are dropped.

Claim 28, and claims 29-30 depending therefrom, are directed to a method for generating filters for network flow and are submitted as patentable for the reasons discussed above with respect to claim 1.

III. Conclusion:

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 446-8695.

Respectfully submitted,

Cindy S. Kaplan
Reg. No. 40,043

RITTER, LANG & KAPLAN LLP
12930 Saratoga Ave., Suite D1
Saratoga, CA 95070
Tel: 408-446-8690
Fax: 408-446-8691